

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA

v.

VINCENT KIEJZO,

Defendant.

CRIMINAL ACTION
NO. 4:20-40036-TSH

**ORDER AND MEMORANDUM ON DEFENDANT’S MOTION TO SUPPRESS AND
FOR A *FRANKS* HEARING (Docket No. 172) AND FOR A RECONSIDERATION OF
HIS MOTION TO COMPEL (Docket No. 189)**

3/21/2023

HILLMAN, S.D.J.

The defendant, Vincent Kiejzo, is charged with possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). He moves to suppress evidence, for a *Franks* hearing, and for a reconsideration of the denial of his motion to compel. For the reasons discussed below, those motions are ***denied***.

Background

On September 8, 2020, Homeland Security Investigations Agent Caitlin Moynihan submitted an application for a warrant to search the defendant’s house for evidence of violations of 18 U.S.C. §§ 2252A(a)(2) and (b)(1) and 2252A(a)(5)(b) and (b)(2), relating to attempted receipt and possession of child pornography. (Docket No. 80-6, at ¶ 4). It is useful in this case to review the affidavit in the order it was written, and therefore as it was presumably read by the issuing magistrate judge.

Agent Moynihan begins with the broad strokes of the investigation: an IP address associated with a certain street address had accessed two websites—“Website 2” and “Website 3”¹ dedicated to child pornography and child sexual abuse materials. (*Id.* at ¶ 5). Agent Moynihan avers that the information in the affidavit comes from United States law enforcement as well as foreign law enforcement agencies (“FLAs”). (*Id.* at ¶ 3).

The affidavit describes both websites as operating on the Tor network, noting that “traditional IP address-based identification techniques are not effective” in locating the users of such websites (*Id.* at ¶ 7). Furthermore, these websites were “hidden” in that they were only accessible via Tor. (*Id.* at ¶ 12). Moynihan explains that Tor is not indexed in the same way as the “standard” internet is by search engines, and therefore it is much more difficult to perform a “Google-type search . . . for particular content of interest.” (*Id.* at ¶ 14). Users interested in child pornography websites on Tor maintain and use “directory sites” that catalogue and advertise those types of sites. (*Id.*). Both Website 2 and Website 3 were listed on directories that advertised child pornography. (*Id.*).

The affidavit contains what appear to be first-hand descriptions of the type of content found on Website 2 and Website 3. (*Id.* at ¶¶ 15-29). The affidavit also describes the process of accessing the content, including that users had to register to view posts on Website 2, (*id.* at ¶ 17) and Website 3 (*id.* at ¶ 24). Agent Moynihan avers that:

Website 2 was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately at least September 2016 to June 2019. In June of 2019, a computer server hosting **Website 2**, which was located outside the United States, was seized by a foreign law enforcement agency.

¹ For reasons not known to this Court, there is never a reference to “Website 1”; as in previous motions in this case, the Court follows the naming convention in Agent Moynihan’s affidavit.

(*Id.* at ¶ 15). A substantially identical paragraph appears prior to the descriptions of Website 3.

(*Id.* at ¶ 23). The FLA in this paragraph will be referred to as the “seizing FLA.” The affidavit continues:

In August 2019, a foreign law enforcement agency (hereinafter, “FLA”) known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that the FLA had determined that on May 12, 2019 at 19:10:51 UTC, [IP address] was used to access online child sexual abuse and exploitation material via a website that the FLA named and described as Website 2.

(*Id.* at 31). A substantially identical tip occurred for Website 3, though the IP address accessed the website at a different time on the same day. (*Id.* at ¶ 32). The FLA in these paragraphs will be referred to as the “notifying FLA.”

Agent Moynihan averred that the notifying FLA had an “established rule of law,” that the information was discovered pursuant to a “lawfully authorized” investigation, and that the notifying FLA had maintained it did not conduct a search of any computer in the United States to obtain the information. (*Id.* at ¶ 33). She further averred that U.S. law enforcement did not participate in the investigative work, and that prior, similar tips had led to arrests, rescuing of children, and seizure of evidence of child pornography trafficking and possession that were determined to be the targets of pending U.S. investigations. (*Id.* at ¶¶ 33-34).

Based on her knowledge of Tor, Agent Moynihan concluded that “it is extremely unlikely that any user could simply stumble upon **Website 2** or **Website 3** without understanding their purpose and content.” (*Id.* at ¶ 37). Law enforcement also obtained via a subpoena information that connected the IP address to defendant’s home and conducted surveillance establishing that he lived there. (*Id.* at ¶¶ 39-47). Agent Moynihan further averred that the information was not stale because collectors of child pornography often keep extensive collections for many years or delete and then reacquire child pornography on a cyclical basis. (*Id.* at ¶¶ 48-57).

On September 8, 2020, a warrant was issued, which was executed the next day. The defendant was found to have a collection of child pornography and was arrested and later indicted on one count of possession of child pornography.

Analysis

1. Probable Cause

The defendant argues that the affidavit in support of the warrant did not support a finding of probable cause that a crime was committed, thus the fruits of the search must be suppressed. When reviewing the issuance of a search warrant by a magistrate judge for probable cause, this Court must give significant deference to that evaluation, “reversing only if we see no substantial basis for concluding that probable cause existed.” *United States v. Cordero-Rosario*, 786 F.3d 64, 69 (1st Cir. 2015) (citations omitted). The defendant puts forward two arguments: the tip from the notifying FLA did not provide a sufficient basis on which to find probable cause and the tip was stale.

a. The Sufficiency of the Tip

The defendant argues that the notifying FLA is akin to a confidential informant and should be analyzed under that framework. In the First Circuit, when an affidavit relies on a confidential informant, “the affidavit must provide some information from which a magistrate can credit the informant’s credibility.” *United States v. Gifford*, 727 F.3d 92, 99 (1st Cir. 2013). In determining an informant’s credibility, the court considers:

(1) whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information; (2) whether an informant's statements reflect first-hand knowledge; (3) whether some or all of the informant's factual statements were corroborated wherever reasonable or practicable (e.g., through police surveillance); and (4) whether a law enforcement affiant assessed, from his professional standpoint, experience, and expertise, the probable significance of the informant’s provided information.

United States v. Tiem Trinh, 665 F.3d 1, 10 (1st Cir. 2011 (citations omitted)). The defendant argues that factors (1), (2), and (3) all go against the government. He argues that the affidavit does not establish the “basis of knowledge,” that it does not reflect “firsthand knowledge,” and that the information was never corroborated.

This Court agrees with the defendant that existing confidential informant case law is relevant to determining the credibility of an anonymous FLA. However, *Trinh* is explicit that its list of factors is not exhaustive. *Id.* If the FLA is from a country without an established rule of law, without a relationship with the United States, and without a history of giving tips that lead to convictions, then the government will likely have to corroborate that information and explain in detail the methodology used. In contrast, when the country has an established rule of law, a relationship with the United States, and a history of fruitful law enforcement collaboration, less information is required. In analyzing tips from FLAs, the analysis is on a spectrum—the more credible the FLA, the less the other factors in the *Trinh* analysis need to be satisfied.

Here, the defendant is correct that the first three factors cut against the government. The “corroboration” mostly consisted of identifying who lived at the physical address connected to the IP address. This corroboration of innocent activity does not help establish probable cause. *Cf. United States v. Greenburg*, 410 F.3d 63, 69 (1st Cir. 2005). Furthermore, the government concedes that it has no idea how the information was collected, so neither the magistrate judge nor this Court has any basis on which to judge the reliability of the tip outside the reliability of the country the notifying FLA came from.

The Court is wary of a practice by which the government might take a “see no evil” approach to working with FLAs, even reliable ones, because it is difficult to access this information within the confines of the Fourth Amendment. However, the Court is also cognizant

of the international and anonymous nature of these crimes. Ultimately, the Court may only overturn a magistrate judge's evaluation if there is "no substantial basis for concluding that probable cause existed." Under that deferential standard, the magistrate judge did not err in crediting the tip given the notifying FLA came from a country with a rule of law, the investigation was conducted according to the country's laws, and past tips had resulted in arrests, seizures, and rescues.

b. The Staleness of the Tip

Defendant argues that the sixteen-month period between the tip and the warrant could only be justified if the government can show it had some basis for believing that he was a collector of child pornography. Because such a basis does not exist, he argues, the tip was stale and could not be the basis for a warrant. The defendant is wrong on both counts.

The First Circuit has held that more than *three years* is not stale in child pornography cases because perpetrators tend to keep their collections. *United States v. Morales-Aldahondo*, 524 F.3d 115, 119 (1st Cir. 2008). This comports with Agent Moynihan's findings. (Docket No. 80-6, at ¶¶ 48-57). The First Circuit does not support defendant's position that the government must present individualized proof that he did not merely stumble upon the content in question. The out-of-circuit case law defendant cites is distinguishable.

In *United States v. Raymonda* the Second Circuit held that a single instance of accessing child pornography can be evidence the suspect is a collector, and thus grounds for a warrant, where "the suspect's access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files." 780 F.3d 105, 115 (1st Cir. 2015). In that case, the Second Circuit found there was insufficient evidence of the defendant being a collector based on the ease of stumbling onto the website in question. But there, a police

officer *also* stumbled across that website, which was not a “hidden website.” *Id.* at 117. Here, the defendant accessed two different “hidden” websites dedicated to child pornography on one day. There is no evidence of other people stumbling across these websites. As discussed below, it is not impossible to stumble upon websites using Tor, but it is more difficult to do so than on the “standard” internet. Therefore, the Court finds that the government had sufficient evidence to suspect that the access was willful. Thus, the sixteen-month tip was not stale.

The motion to suppress based on a lack of probable cause is *denied*.

2. *Franks* Hearing

A *Franks* hearing is only justified if the defendant makes “a substantial preliminary showing” that the statements were “knowingly and intentionally [false], or [made] with reckless disregard for the truth,” and that the falsehood was “necessary to the finding of probable cause.” *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). Intentional or reckless omissions are also relevant if “the omitted information, if incorporated into the affidavit, [are] sufficient to vitiate probable cause. *United States v. Tanguay*, 787 F.3d 44, 49 (1st Cir. 2015).

a. *Omissions or Misrepresentations About the Nature of Tor*

Defendant argues that the affidavit implies that it is impossible, or extraordinarily unlikely, for an innocent user to “stumble upon” child pornography when using Tor. He presents an affidavit from another case which presents a contrary view. That affidavit asserts that it is easy to find “links” on Tor by conducting a “simple search.” The affidavit further notes that “[t]he typical names of these hidden Tor websites do not indicate possible content, due to the use of the 16-or-56-character web address.” (Docket No. 172, at 26).

The defendant has not made a strong preliminary showing of misrepresentation. The defendant’s affidavit represents that it is relatively easy to find links on Tor. The government’s

affidavit represents that, given the nature of Tor, it is unlikely that defendant stumbled upon two hidden child pornography websites in one day. “[I]t is extremely unlikely that any user could simply stumble upon **Website 2** or **Website 3** without understanding their purpose and content.” (Docket 80-6, at ¶ 37). Those statements are not contradictory. At most, they represent a disagreement about the likelihood of stumbling upon websites using Tor, not that it is impossible. Because there is no misrepresentation, this theory fails.

b. Misrepresentations About the Nature of the Tip

First, defendant argues the affiant changed language in the tip from the notifying FLA when describing the tip in the affidavit. He claims that change misled the magistrate judge into thinking that the user at the IP address had accessed illegal material, when the tip only showed that the user at the IP address had accessed the websites. Those websites did not allow non-users to access materials and had no illegal material on their home pages, thus the defendant argues that the original tip did not prove the user actually accessed illegal material.

It is useful to quote the language from the affidavit and the tip. The relevant section of the affidavit states:

on May 12, 2019 at 19:10:51 UTC, [IP address] was used to access online child sexual abuse and exploitation material *via a website* that the FLA named and described as Website 2. FLA . . . stated that users were required to create an account (username and password) in order to access the majority of the material, and provided further documentation naming the website as Website 2, which the FLA referred to by its actual name.

(Docket 80-6, at ¶ 31) (emphasis added). The defendant argues the exact words of the tip are, in relevant part:

On 2019-05-12 19:10:51 (UTC) [IP address] was used to access online child sexual abuse and exploitation material [description omitted]. Users were required to create an account (username and password) in order to access the majority of the material[.]

(Docket 172, at 16). Defendant insists that inserting the words “via a website” materially misled the magistrate judge. But the tip does not make a distinction between the website and the material. Removing the offending words does not affect the meaning of the affidavit: “the FLA had determined that on May 12, 2019 at 19:10:51 UTC, [IP address] was used to access online child sexual abuse and exploitation material.”

The defendant further argues that Agent Moynihan knew the tip meant something other than what the affiant related. When the tip *said* “[IP address] was used to access online child sexual abuse and exploitation material” the affiant allegedly knew that it *meant* “[IP address] was used to access the website.” Thus, Agent Moynihan should have used the latter formulation, even if it was not the formulation the actual tip used.

Defendant points to an investigative report by the notifying FLA that uses “identical language” to the tip in describing the website, not the user’s access. Similarly, the defendant argues language from earlier in Moynihan’s affidavit that the user “accessed Website 2 and Website 3” as proof the government knew the plain language of the tip was erroneous. But that language is consistent with the tip—that the defendant accessed illicit materials *via* the website. This is not enough to make a “substantial preliminary showing” of misleadingness.² Because there is no misrepresentation, the theory fails.

c. Omissions about the Origin of the Tip

Defendant also argues that the United States omitted that the servers were seized not by the notifying FLA, but the seizing FLA, because the affidavit never explicitly identifies the FLAs as distinct. He argues this is material because the affidavit implies the two FLAs are one and the

² Defendant also argues that this change somehow led the magistrate judge to not understand that the homepages contained no illicit material. As the background section makes clear, Agent Moynihan’s affidavit is clear that a user must register to view unlawful material on both sites.

same and therefore no credibility determination was made as to the seizing FLA's reliability or rule of law. The question is whether "the omitted information, if incorporated into the affidavit, [is] sufficient to vitiate probable cause." *Tanguay*, 787 F.3d at 49.

The identity of the seizing FLA was omitted from the application. The defendant has purported to identify the seizing FLA, which is different than the notifying FLA, and the government neither confirms nor denies that assertion. The seizing FLA identified by the defendant is a democracy, though it does not seem to have the long-term law enforcement relationship with the United States that the notifying FLA has nor the same rule of law credentials.

This Court does not agree that Moynihan's affidavit implies that the FLAs are one and the same; at best it is ambiguous. The references to the FLAs appear eight paragraphs apart. When the notifying FLA is first mentioned, it is not referred to as the "previous" FLA nor is there any indication they are the same. Indeed, it is only after the notifying FLA is first mentioned that the affidavit identifies it as "FLA," rather than "foreign law enforcement agency," indicating all subsequent references are to the notifying FLA.

As to the second allegation, a credibility determination is only necessary if the FLA provided the United States with information. There is no indication in the affidavit that the seizing FLA provided any information to the United States. A fair reading of the affidavit indicates that the seizure of the server is mentioned solely to explain why the websites shut down.

In a supporting memorandum, defendant purports to show that the seizing FLA provided the IP address information to the notifying FLA, which then passed on the information to the United States. But the document defendant provides does not support that theory. The document

alleges the seizing FLA gave “information” to other countries after seizing the server that hosted the websites in question. But the sealed exhibit describes the notifying FLA providing IP addresses *to the seizing FLA*. If anything, this supports the government’s contention that the notifying FLA, not the seizing FLA, was the source of the tip here. Indeed, the United States argues the notifying FLA could not have extracted his IP address from the server post-seizure because the defendant accessed the server prior to the seizure and his address would have been masked due to the nature of the Tor service. Under both the United States’ and the defendant’s representations, the notifying FLA must have used some “contemporaneous” method of tracking the IP addresses that accessed the server that was eventually seized.

Because there is no evidence the seizing FLA provided information to the United States, the omission of its identity is not material and this theory fails.

d. Omissions and Misrepresentations about the Method the Notifying FLA Used to Identify the IP Address.

Defendant argues, via an affidavit from a cybersecurity researcher, that there are only two ways the notifying FLA could have obtained the IP address. First, they might have used “[t]raffic analysis,” which defendant argues is unreliable and therefore cannot be the basis for a finding of probable cause. Second, they might have used a “Network Investigative Technique” (“NIT”), which requires some control of the website because it consists of sending malware to computers that access the website to unmask their identity. There is precedent suggesting that an NIT is a search for Fourth Amendment purposes. *United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass. 2016). The defendant argues that the United States knows the technique used by the notifying FLA and that, in any case, the United States knew that computers in the United States were searched.

In support of their first theory, defendant cites a motion to redact a probable cause affidavit in a different district where the government argued that some investigatory technique needed to remain under seal. Other than that case also being a child pornography case, this Court is unable to locate any information that shows it is “related” to the instant case. Thus, there is no reason to think that the technique used in *this* case to obtain the IP address is the same as the technique used in *that* case.

Defendant’s second argument is stronger. While he has not shown that the United States knew of the technique used and therefore has not established that it knew the technique was a search for Fourth Amendment purposes, he has established that United States at least had reason to know that there was a search. Although a single affidavit by a cybersecurity researcher in a different case is a thin reed on which to make a “substantial preliminary showing,” the United States has taken the position in responding to defendant’s motion that it is not possible for IP addresses to be retroactively extracted from a seized Tor server. That at least supports, even if it does not confirm, the defendant’s theory that his IP address was identified by something like an NIT—which is likely a search under the Constitution. Thus, the United States had reason to know that there was likely a search of a computer in the United States.

The affidavit states that the notifying FLA has “advised . . . that [it] had not interfered with, accessed, searched, or seized any data from any computer in the United States”; it does not technically contain an assertion by the United States that it *believes* the notifying FLA. However, there is no reason for the United States to include this assertion in its application for a warrant if it does not believe it to be truthful. It might be that the notifying FLA did not understand its methods to be a search. But in that case, including its statement without context becomes a lie of omission.

However, even if there was a misrepresentation, it is not material. As discussed below, searches conducted by FLAs are not subject to the exclusionary rule, even when they are conducted on American “soil.” The exclusionary rule is intended as a deterrence mechanism, and that deterrence mechanism would have little effect on foreign countries. *United States v. Hensel*, 699 F.2d 18, 25 (1st Cir. 1983). So long as the search came from a credible partner, was not done in concert with the United States, and does not shock the conscience, the fruits of searches of Americans by FLAs may be used to support an application for a warrant. That there was likely a search is not, in and of itself, material. Therefore, this theory fails.

e. The Exclusionary Rule

Normally, evidence discovered by foreign governments is not subject to the exclusionary rule even if the means of discovery would have been unconstitutional if undertaken by the United States without a warrant. There are two exceptions: when the search is the result of a “joint venture” between the United States and the FLA or when the methods used by the FLA “shock the conscience.” *United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). The defendant argues that he has made a preliminary, substantial showing that the government was engaged in a joint venture with the notifying and/or seizing FLA and that the purported method would “shock the conscience.”

i. Joint Venture

In the First Circuit, courts consider several factors in determining whether there was a “joint venture” including:

- (1) whether American authorities initiated the investigation in the foreign country;
- (2) whether American authorities were involved in the decision to seek the foreign [search];
- (3) whether American agents controlled, directed, or supervised the foreign [search]; and
- (4) whether American agents participated in “the implementation of the [search].”

United States v. Marte, 2018 WL 4571657, at *6 (D. Mass. Sept. 24, 2018) (citing *Valdivia*, 680 F.3d at 52). To prove his joint venture theory, defendant catalogues cooperation between the government and various foreign countries (though not the country the notifying FLA is located in)³ in tracking child pornography websites over several years, including the websites that defendant accessed. He also presents evidence that the United States had access to a “searchable copy” of one of the websites. But that does not describe a cohesive investigation—it describes several investigations, over many years, which may overlap. As Agent Moynihan’s affidavit makes clear, investigating these websites offer few clues to law enforcement as to who accessed them. (Docket No. 80-6, at ¶ 30).

Defendant also argues that he has discovered recent criminal cases across the country that rely on a tip nearly identical to the one used to justify the warrant in his case, proving a joint venture. The United States tacitly acknowledges there are similar contemporaneous cases. *See generally United States v. Bateman*, No. 20-CR-10012-IT, 2021 WL 3055014 (D. Mass. July 20, 2021). What defendant has discovered is not a joint venture, but an investigation conducted by the notifying FLA. Defendant’s research confirms what Agent Moynihan’s affidavit revealed to the magistrate judge:

when a law enforcement agency obtains evidence that such a [child pornography] website or user may be located in another country, *it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the site is located or the offender appears to reside.*

(Docket No. 80-6, at ¶ 30) (emphasis added).

It would be strange if the notifying FLA, in investigating an English language website with “over 310,000 members and over 4.1 million postings,” (*id.* at ¶ 23), only identified a single American user. The test, as described above, is not about vague allegations of cooperation, but

³ The parties and the Court are aware of the identity of the notifying FLA.

the degree of control and participation United States law enforcement had in the search. *United States v. Acevedo-Martinez*, No. 14-cr.754-DRD, 2020 WL 2537644, at *9 (D.P.R. May 18, 2020) (finding no joint venture where United States law enforcement cooperated with the FLA, shared information, and participated in arrest of defendant).

In supporting memorandum, defendant offers more of the same. First, he points out that there was an international investigation in 2017 by the seizing FLA that resulted in the arrest of two administrators of a child pornography site not at issue in this case. For the reasons above, that has no bearing on this case. More relevantly, he alleges that the United States was involved in the seizure of the server from which the IP address of the defendant was allegedly identified.

First, he alleges that the United States confirmed the identity of the individual who hosted the servers as a known criminal who purveyed child pornography to the seizing FLA. Second, the seizing FLA, with the help of an informant and technical assistance from the United States in the form of a “deanonymization technique,” was able to identify the IP address of the owner of the server. To be clear, the technique described by the defendant “deanonymizes” people who *host* servers that, in turn, host content on Tor—it does not deanonymize *user’s* IP addresses when they access servers, like the defendant. With authorized telephone wiretaps, the seizing FLA was able to confirm the presence of the server and, eventually, to seize it. No further help by United States law enforcement is alleged. Although the defendant alleges information was shared with the United States, the document only indicates that information was shared by the seizing FLA with other countries, and the specific countries it does indicate do not include the United States—though they do include the notifying FLA. As discussed above, the defendant’s theory is that the notifying FLA somehow extracted the defendant’s IP address after being given information by the seizing FLA.

First, that is inconsistent with his theory that only NITs—which unmask Tor users by tracking them contemporaneously with their access of servers—could identify him. Even so, this Court will assume without deciding that the seizure of the server, the collection of IP address information, and the transmission of that information to the United States is a single “investigation” for the purposes of the joint venture doctrine. Turning to the factors from *Valdivia*, defendant offers no evidence that the investigation was instigated by the United States. Instead, at a few points the seizing FLA requested, and received, assistance from the United States. He offers no evidence United States law enforcement was involved in the decision either to seize the server or to find the IP addresses, or that the United States controlled, directed, or supervised either the decision to seize the server or the searches for the IP addresses. Because this was not a joint venture, there was no misrepresentation and the theory fails.

ii. Shocks the Conscience

As to the “shock’s the conscience” theory, defendant argues that because using an NIT without a warrant is an unlawful search, it shocks the conscience. This is premised on defendant’s theory that only an NIT could have uncovered the defendant’s IP address.

“Circumstances that will shock the conscience are limited to conduct that ‘not only violates U.S. notions of due process, but also violates fundamental international norms of decency.’” *United States v. Mitro*, 880 F.2d 1480, 1483-84 (1st Cir. 1989) (citing Stephen Saltzburg, *The Reach of the Bill of Rights Beyond the Terra Firma of the United States*, 20 Va. J. Int’l. L. 741, 775 (1980)). The First Circuit has held that the use of an NIT by the government pursuant to a warrant does not shock the conscience. *United States v. Anzalone*, 923 F.3d 1, 5-6 (1st Cir. 2019). This Court does not find that the possible use of an NIT by an FLA, consistent with its own laws, would shock the conscience without more, and defendant has offered nothing

more. Furthermore, the supporting memorandum describes an investigation by the seizing FLA that is punctuated by court authorizations every time law enforcement conducts what would be a search under the United States Constitution. That investigation does not shock the conscience. Because the defendant has not made a substantial preliminary ruling that the exclusionary rule applies, this theory fails.

Therefore, the motion for a *Franks* hearing is *denied*.

3. Motion for Reconsideration

In addition to his supplemental memorandum, defendant moves for reconsideration of this Court's denial of his motion for discovery. For the reasons above, the supporting memorandum does not contain new information that suggests defendant's theories are more plausible. That motion is *denied*.

Conclusion

For the reasons above, the motion to suppress, the motion for a *Franks* hearing, and the motion to reconsider are **denied**.

SO ORDERED

/s/ Timothy S. Hillman
TIMOTHY S. HILLMAN
SENIOR DISTRICT JUDGE